

برامج آبل وخدماتها تتضمن 55 عيبًا أمنيًا



الأحد 11 أكتوبر 2020 02:10 م

حلل فريق مكون من خمسة باحثين أمنيين العديد من برامج شركة آبل وخدماتها عبر الإنترنت لمدة ثلاثة أشهر امتدت بين شهري يوليو وسبتمبر

ووجد الفريق ما يصل إلى 55 نقطة ضعف، 11 منها بالغة الخطر، و 29 منها ذات درجة خطر عالية، و 13 منها متوسطة الخطر، و 2 منها منخفضة الخطر

وقال الفريق: تسمح العيوب للمهاجم بخرق تطبيقات العملاء والموظفين بشكل كامل، وإطلاق برمجية ضارة قادرة على الاستيلاء تلقائيًا على حساب آيكلود للضحية

وأضاف: كما تسمح باسترداد التعليمات البرمجية المصدرة لمشاريع آبل الداخلية، واختراق برنامج مستودع التحكم الصناعي الذي تستخدمه آبل، والتحكم بجلسات موظفي آبل مع إمكانية الوصول إلى أدوات الإدارة والموارد الحساسة

وتعني العيوب أن بإمكان المهاجم اختطاف حساب آيكلود للمستخدم بسهولة وسرقة جميع الصور ومعلومات التقييم ومقاطع الفيديو والمستندات، بالإضافة إلى إعادة توجيه الاستغلال نفسه إلى جميع جهات الاتصال

ويتكون فريق الباحثين من سام كاري (Sam Curry) وبريت بويرهاوس (Brett Buerhaus) وبن صادقيبور (Ben Sadeghipour) وصموئيل إيرب (Samuel Erb) وتانر بارنز (Tanner Barnes).

واتخذت الشركة المصنعة لهواتف آيفون خطوات لإصلاح العيوب في غضون فترة قصيرة بعد أن تم الكشف عنها بشكل مسؤول لشركة آبل

وعالجت آبل حتى الآن نحو 28 من نقاط الضعف، ودفعت مبلغًا إجماليًا يصل إلى 288500 دولار كجزء من برنامج مكافآت الأخطاء

وسمح أحد نطاقات آبل المتأثرة (ade.apple.com) بتجاوز المصادقة باستخدام كلمة مرور افتراضية، مما أتاح للمهاجم الوصول إلى وحدة تحكم المسؤول وتنفيذ التعليمات البرمجية

وتسبب خلل مرتبط بتطبيق يسمى (DELMIA Apriso)، وهو حل لإدارة المستودعات، في السماح بتعديل الشحنات ومعلومات المخزون والتحقق من صحة شارات الموظفين والسيطرة الكاملة على البرنامج

وتم اكتشاف ثغرة أمنية منفصلة أيضًا في خدمة (Apple Books for Authors) التي يستخدمها المؤلفون للمساعدة في كتابة ونشر كتبهم عبر منصة (Apple Books).

ومن بين المخاطر الهامة الأخرى التي كشف عنها الباحثون تلك التي نشأت عن ثغرة في البرمجة النصية عبر المواقع (XSS) في مجال (www.icloud.com).

وكانت ثغرة (XSS) قابلة للنشر بسهولة عن طريق إرسال بريد إلكتروني مشابه إلى كل عنوان (iCloud.com) أو (Mac.com) مخزن في جهات اتصال الضحية

وقال الفريق في تدوينه: لم تكن لدينا أي فكرة عندما بدأنا هذا المشروع لأول مرة أننا سنقضي ما يزيد قليلاً عن ثلاثة أشهر في العمل على استكمالهِ

وأضاف: كان من المفترض أن يكون هذا في الأصل مشروعًا جانبيًا كنا نعمل عليه من حين لآخر، وخصصنا للمشروع بضع مئات من الساعات